UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

212 S Univeristy Dr. #6, West Bend, WI 53095; silver 2018 Buick, VIN KL4CJCSB0JB524629, WI plate ANG1780; person of Brandon Gerry, DOB 12/5/1984; (See Attachments)

Case No. 23 MJ 52

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252(a)(2)	Receipt/distribution/transportation of child pornography
18 U.S.C. 2252(a)(4)(B).	Possession of child pornography

The application is based on these facts:

See Attached Affidaivt

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Sarah Dettmering, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 2/27/2023

Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Sarah Dettmering, being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since January 2018 and am currently assigned to the Milwaukee Division as a member of the Milwaukee Child Exploitation and Human Trafficking Task Force. My duties include investigating criminal violations relating to child sexual exploitation and child pornography. While employed by the FBI, I have investigated federal criminal violations related to complex financial crimes, health care fraud, cybercrimes, child exploitation, and child pornography.

2. I have received training from the FBI specific to investigating child pornography and child exploitation crimes and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256) in different forms of media including computer media. As a result of my training, experience, and discussions with other law enforcement officers assigned to investigate child pornography and child exploitation, I am familiar with methods by which electronic devices are used as the means for receiving, transmitting, possessing, and distributing images and videos depicting minors engaged in sexually explicit conduct. I have also received training and gained experience in interview and interrogation techniques with enhanced training specific to cybercrimes, social media search warrants, residential search warrants, interviews and interrogations of subjects of criminal investigations, electronic device identification and forensic review.

3. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, and through information provided to me by other law

enforcement officers, who have provided information to me during the course of their official duties and whom I consider truthful and reliable.

4. Based upon the information described below, I submit that probable cause exists to believe that Brandon Gerry has committed multiple violations of distribution of child pornography in violation of Title 18, United States Code, Section 2252(a)(2), and possession of child pornography in violation of Title 18, United States Code, Section 2252(a)(4)(B) while residing at 212 S UNIVERSITY DR, APT 6, WEST BEND, WI 53095 (SUBJECT PREMISES). I further submit that evidence relating to this crime, more particularly described in Attachment B, can be found at the SUBJECT PREMISES, in a silver 2018 Buick, VIN KL4CJCSB0JB524629, Wisconsin license plate ANG1780 (SUBJECT VEHICLE), and on the person of Brandon Gerry (GERRY) more particularly described in Attachment A. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

DEFINITIONS

5. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

- "Child Pornography" is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

- "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

- The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

- An "Internet Protocol address" (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static that is, long-term IP addresses, while other computers have dynamic that is, frequently changed IP addresses.

- "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

- The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion

pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

- "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

- "Visual depictions" include undeveloped film and videotape, and data stored on a computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

- "Website" consists of text pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol.

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

6. I am aware through training, experience, and consulting with other law enforcement agents/analysts with specialized knowledge and training in computers, networks, and Internet communications that to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from

accidental or programmed destruction, it is necessary to conduct a forensic examination of the electronic storage devices. To ensure such accuracy and completeness, it may also be necessary to analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, other storage media, within a hand-held electronic device such as a cellular telephone or a tablet device (e.g., an iPad device). Some of this electronic information, as explained below, might take a form that becomes meaningful only upon forensic analysis.

7. Based on my knowledge, training, and experience, I know that computer and other electronic device hardware, peripheral devices, software, documentation, and passwords may be important to a criminal investigation in three distinct and important respects:

a. The objects themselves may be instrumentalities used to commit the crime.

b. The objects may have been used to collect and store information about crimes (in the form of electronic data).

c. The objects may be contraband or fruits of the crime.

8. I submit that if a computer or other electronic storage device is found on the premises, there is probable cause to believe those records will be stored in that electronic storage device, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person deletes a file on an electronic storage device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. It follows that deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone, or tablet device) the device may also contain a record of deleted data in a swap or recovery file.

b. Wholly apart from user-generated files, electronic storage device storage media in particular, computers' internal hard drives, contain electronic evidence of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, and file system data structures. Electronic storage device users typically do not erase or delete this evidence because special software is typically required for that task. However, it is technically possible to delete this information.

c. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or cache. The browser often maintains a fixed

amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

9. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how electronic storage devices were used, the purpose of their use, who used them, and when.

10. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), electronic storage device storage media can contain other forms of electronic evidence as described below:

a. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within an electronic storage device and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion.

In my training and experience, information stored within an electronic storage device (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic storage device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic storage device was remotely accessed, thus inculpating or exculpating the electronic storage device owner. Further, electronic storage device activity can indicate how and when the electronic storage device was accessed or used. For example, as described herein, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera). The geographic and timeline information described herein may either inculpate or exculpate the electronic storage device user. Last,

information stored within an electronic storage device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic storage device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user's knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner.

11. Based upon my knowledge, training and experience, and after having consulted with FBI computer forensic personnel, I know that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a

controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some electronic storage device equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how an electronic storage device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Electronic storage devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of electronic storage device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to

analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

12. In light of these concerns, I hereby request the Court's permission to seize the electronic storage devices, associated storage media, and associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the hardware, media, or peripherals on-site for this evidence.

13. I know that when an individual uses a computer to commit crimes involving child pornography, the individuals' computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage device is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe that an electronic storage device used to commit a crime of this type may contain data that is evidence of how the electronic storage device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

BIOMETRIC ACCESS TO DEVICES

14. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

15. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

16. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.

Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

17. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

18. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

19. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

20. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

21. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, I request authority for law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of GERRY, or any of the residents of the SUBJECT PREMISES to the fingerprint scanner of the devices found on GERRY or at the SUBJECT PREMISES or in the SUBJECT VEHICLE; (2) hold the devices found on GERRY, in the SUBJECT VEHICLE or at the SUBJECT PREMISES in front of the residents' face to activate the facial recognition feature; and/or (3) hold the devices found on GERRY, in the SUBJECT VEHICLE or at the SUBJECT PREMISES in front of the residents' face and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

BACKGROUND ON NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

22. Based on my training and experience, and publicly available information, I know that the National Center for Missing and Exploited Children (NCMEC) is a nonprofit organization in Alexandria, Virginia, that works with law enforcement on issues related to missing and sexually exploited children. One of the services provided and administered by NCMEC is its CyberTipline, which serves as the national clearinghouse for leads regarding sexual exploitation crimes against children.

23. In addition to reports from the general public, reports are made by U.S. electronic communication service (ECS) providers and remote computing services (RCS), which are required by 18 U.S.C. § 2258A to report "apparent child pornography" to NCMEC via the CyberTipline if they become aware of the content on their servers. Specially trained analysts, who examine and evaluate the reported content, review leads, add related information that may be useful to law enforcement, use publicly available search tools to determine the geographic location of the apparent criminal act, and ultimately provide all of the gathered information to the appropriate law enforcement agency for review and possible investigation.

24. The CyberTipline receives reports, known as CyberTips, about the possession, production and distribution of child pornography; online enticement of children for sexual acts; child sex trafficking; sex tourism involving children; child sexual molestation; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet.

25. The CyberTip reports will vary in detail depending on the nature of the report, and which entity submits it. The reports can include information (1) relating to the identity of any

individual who appears to have violated federal law by committing or attempting to commit the criminal conduct described above; (2) historical information on when or how a customer or subscriber of an ECS or RCS uploaded, transmitted, or received apparent child pornography; (3) geographical information on the involved individual or website, which may include the IP Address or verified billing address or geographic identifying information, including area code or zip code; (4) any images of apparent child pornography; and (5) the complete communication containing any image of apparent child pornography.

BACKGROUND ON DISCORD

26. Discord is a messaging platform where millions of users from around theworld connect with each other through chat, voice, and video. Discord has both a desktop (PC, Mac, Linux) application and a mobile (iOS, Android) application, and the service can also be accessed from the website directly at www.discordapp.com.

27. In order to use the services, users need to create an account by selecting a username. Once they've made their account, users can create a server and invite their friends to join it with an invite link, or they can join an existing server. Servers are broken down into sub-categories or "channels" where users can connect with each other by either chatting or calling. Users can also communicate through direct messages, which are private chats created between 1-10 users.

28. To create a Discord account, the user is also required to provide an email address which is verified by Discord.

29. Providers like Discord, Inc. typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on

which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the subject's account.

30. In some cases, Discord users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

BACKGROUND ON MEWE

31. MeWe is a social networking site which can be accessed through the URL: https://mewe.com/. MeWe is a social network which emphasizes social sharing where people can be their "true, authentic selves." MeWe is available on iOS, Android, and desktop. The service provides the ability to chat, connect with friends and family, provide newsfeeds, private1:1 and group chatting, disappearing content, a camera with Gif creation, live voice and live video, next-gen voice messaging, secret chats with double-ratchet encryption, a personal social cloud, and a "My Cloud." "My Cloud" can be used to organize content and provide the user with an interactive dashboard to control everything the user has posted or shared, making it simple to delete or reshare.

32. MeWe's Terms of Service, which is publicly available on their website state:

- When you use our Services, we process any data you explicitly enter into the site (your "Content Data"), including your full name, email address, profile information, posts, comments, photos, voice recordings, videos, files, emojis, etc. MeWe uses your Content Data for the sole purpose of serving and providing you with the full experience of MeWe. You control how we process your Content Data through Privacy & Sharing settings in your account at MeWe. At any time you can edit/update, retrieve or delete your Content Data in your account.

- When you use our Services, we may receive information ("Log Data") such as your IP address, browser type, operating system, the referring web page, pages visited, location, your mobile carrier, and device information (including device and application IDs). We receive Log Data when you interact with our Services, for example, when you visit our websites, sign into our Services, interact with our email notifications, use your account to authenticate to a third-party website or application. We may also receive Log Data when you click on, view or interact with links on our Services, including links to third-party applications, such as when you choose to install another application through MeWe. MeWe uses Log Data to provide, understand, and improve our Services. We either delete Log Data or remove any common account identifiers, such as your username, full IP address, or email address, after a maximum of 12 months.

BACKGROUND ON REDDIT

33. Reddit is a community of online communities (known as "subreddits" or "subs") organized around the shared interests of their members.

34. Each subreddit has its own page, subject matter, users, and volunteer moderators (also known as "mods"). Community members interact within these subreddits by posting topical

information, articles, stories, links, news, images, and videos, which are then voted and commented upon by Reddit account holders. The number of upvotes and downvotes a post receives helps determine its position within the subreddit.

35. Reddit may be accessed via Reddit.com, or through associated mobile applications (e.g., Reddit for Android, Reddit for iOS).

36. Reddit generally collects minimal information from users and may have little or no non-public information available for many accounts. Reddit.com users are not required to provide their name or contact information (including email address), though users can choose to provide their email address. Reddit does not automatically verify the information provided by its users, though users may choose to verify their email address. Users may also choose to register Reddit accounts via single sign-on (SSO) using their existing Google or Apple accounts.

37. Reddit account information is generally separated into four categories:

- **Basic Subscriber Information** - This includes the username/subscriber identity, IP logs (including registration IP), the user's name (if any), email address (if any), and phone number (if any).

- **Other non-content records about the user or the user's conduct on Reddit** - This includes user preferences and communication headers (e.g., the to/from fields of a Private Message or the participant list for a chat discussion).

- **Content of Communications (public)** - This includes posts, comments, and other information regarding the substance of a user's publicly available communications. This content is publicly available without Reddit, Inc.'s assistance.

- **Content of Communications (non-public)** - This includes non-public messages/communications between users, information about a user's votes, posts, comments, and other information regarding the substance of a user's communications across Reddit.

38.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

Discord

39. On or about January 25, 2023, NCMEC received a Cybertip from Discord, Inc. Discord, Inc. provided the following identifiers for the associated subject Discord account, the SUBJECT ACCOUNT 1:

- Telephone number: 414-488-4501
- E-mail address: gerrybr1681@gmail.com
- Username: stevegay#6225
- User ID: 1064583564840149085

40. Discord, Inc. provided the following information related to the uploaded file, which prompted Discord, Inc. to file the Cybertip:

- Filename: VID_20230123_200347_460.mp4
- MD5 (Hash Value): a84c9758c070619dc964acbafb634799
- Upload Date/Time: 01-25-2023 21:09:33 UTC
- Upload IP Address: 35.148.74.1

41. Discord, Inc. provided the above-described video with the submitted Cybertip. I reviewed the video and determined it is consistent with the definition of child pornography. The video is described as follows:

- The video is approximately two (2) minutes and forty (40) seconds long. The video shows a prepubescent boy, approximately seven (7) to nine (9) years old,

nude from the waist down lying on his side with his leg lifted in the air to expose his penis and buttocks. An older male, approximately fifteen (15) to eighteen (18) is lying behind the boy and is rubbing his nude penis on the boy's buttocks.

42. In my training and experience, if a user uploads or shares one file of child pornography it is likely that they have received or distributed more files.

43. NCMEC performed an automated query on the identifiers provided by Discord, Inc. and found approximately thirteen (13) other Cybertips related to the SUBJECT ACCOUNT's associated email address, and a total of approximately sixteen (16) associated Cybertips.

44. On or about February 7, 2023, T-Mobile was served with an administrative subpoena by an Operational Support Technician with FBI Milwaukee requesting subscriber information for the cell phone number associated with SUBJECT ACCOUNT 1, 414-488-4501. On or about February 14, 2023, T-Mobile provided a response to the administrative subpoena and showed that the subscriber to the cell phone associated with SUBJECT ACCOUNT 1 was the SUBJECT, Brandon Gerry.

45. On or about February 7, 2023, Google LLC was served with an administrative subpoena by an Operational Support Technician with FBI Milwaukee requesting subscriber information for the email address associated with SUBJECT ACCOUNT 1, gerrybr1681@gmail.com. On or about February 9, 2023, Google LLC provided a response to the administrative subpoena, which showed the following information:

- Name: Brandon
- Given Name: Brandon
- Created On: 2023-01-07 22:04:31 Z
- Recovery SMS: +14144307294 [US]
- IP Address/Login: 2600:6c44:66f0:1b0:1907:5a7b:6ee3:e1b7
  - Timestamp: 2023-02-02 21:03:06 Z

- Timestamp: 2023-02-01 03:16:08 Z

46. On or about February 9, 2023, US Cellular was served with an administrative subpoena by an Operational Support Technician with FBI Milwaukee requesting subscriber information for the cell phone number associated with the email account gerrybr1681@gmail.com, +1414-430-7294. On or about February 13, 2023, US Cellular provided the following information for the phone number: +1414-430-7294

- Customer Name: Brandon Richard Gerry
- Subscriber Activation Date/Time: 1/7/2023 3:35:57 PM
- Subscriber Status: Active
- Line Type: Smartphone

47. On or about February 9, 2023, Charter Communications, Inc. (Charter) was served with an administrative subpoena by an Operational Support Technician with FBI Milwaukee requesting subscriber information for the IP Addresses used to login to gerrybr1681@gmail.com. On or about February 15, 2023, Charter provided a response to the administrative subpoena and showed the following subscriber information:

- Subscriber Name: Brandon Gerry
- Service Address: 212 S UNIVERSITY DR, APT 6, WEST BEND, WI 530952980
- Billing Address: 212 S UNIVERSITY DR, APT 6, WEST BEND, WI 530952980
- Username: brgerry1681@gmail.com
- Phone Number: 414-488-4501
- Lease Start Date: 11/09/2023 04:30 AM
- Lease End Date: 02/10/2023 06:15 PM

48. The email address and the phone number associated with GERRY's Charter account are the same email address and phone number associated with the Discord account, SUBJECT ACCOUNT 1.

49. On or about February 7, 2023 Discord, Inc. was served with a Preservation Request for the SUBJECT ACCOUNT 1 by an Operational Support Technician with FBI Milwaukee.

50. On or about February 10, 2023 Discord, Inc. was served with a federal search warrant issued in the Eastern District of Wisconsin for the contents of SUBJECT ACCOUNT 1. On or about February 13, 2023 Discord, Inc. provided records related to SUBJECT ACCOUNT 1 in response to the federal search warrant.

51. I reviewed the contents of the records provided by Discord, Inc. in response to the search warrant and observed images and videos consistent with child pornography, as well as direct messages between SUBJECT ACCOUNT 1 and other accounts where SUBJECT ACCOUNT 1 shared files of child pornography.

52. SUBJECT ACCOUNT 1 was a member of a particular Discord server named "LSX." SUBJECT ACCOUNT 1 shared the video file reported by Discord, Inc.in the Cybertip described above in the server's sub-channel which was titled "\ud83d\udcfc\u2503nsfw-vids." As reported in the Cybertip this video was shared on January 25, 2023.

53. SUBJECT ACCOUNT 1 was a member of a particular Discord server named "stevegay's hole." SUBJECT ACCOUNT 1 shared multiple files consistent with the definition of child pornography in the server's sub-channel which was titled "general."

54. The owner identification number for this server was, 1064583564840149085. This identification number matches the user identification number for SUBJECT ACCOUNT 1, indicating that the user of SUBJECT ACCOUNT 1 created the server.

55. On or about January 16, 2023, at 17:53:42 (+0:00) the SUBJECT ACCOUNT 1 shared a video with the filename: VID_20230115_171525_540.mp4 which I viewed and

determined is consistent with the definition of child pornography. The video is described as follows:

- This is a full color video, approximately twenty-three seconds in length. It shows a prepubescent female, approximately four to six years old, with an adult male's penis inserted in her mouth.

56. On or about January 16, 2023, at 18:56:29 (+0:00) the SUBJECT ACCOUNT 1 shared a video with the filename: VID_20230115_181040_910.mp4 which I viewed and determined is consistent with the definition of child pornography. The video is described as follows:

- This is a full color video, approximately eleven seconds in length. It shows a prepubescent female, approximately six to eight years old, with an adult male's penis inserted in her mouth. The video then shows the girl on her knees on a bed with her buttocks towards the camera, there is a white substance consistent with semen on her buttocks. The video then shows the girl lying nude on her back with her legs spread. An adult male's penis is inserted in her vagina.

57. There were also more than fifteen (15) direct messages in which the SUBJECT ACCOUNT 1 shared both image and video files which I determined to be consistent with the definition of child pornography.

MeWe

58. On or about January 17, 2023, NCMEC received a Cybertip, number 153000256, from MeWe. MeWe provided the following identifiers for the associated subject MeWe account, the SUBJECT ACCOUNT 2:

- E-mail address: gerrybr1681@gmail.com
- Username: Steve Gay
- Login IP Address: 35.148.74.1

59. MeWe provided the filename and MD5 Hash Value for the eleven (11) uploaded image files, which prompted MeWe to file the Cybertip.

60. MeWe provided the eleven (11) image files which were viewed by MeWe and NCMEC that were submitted with the Cybertip. I reviewed the files and determined they were consistent with the definition of child pornography. One of the images is described as follows:

- Filename: i_63c1091dd9fbbd196d75eb15.png
- Incident Date/Time: 1/13/2023 07:32:45 UTC
- MD5 Hash Value: c6d07fab7c0ab8033d9181d575d803fc
- The image is a full color image which shows a nude from the waist down, prepubescent female lying on her back with her legs spread and an adult male between her legs. The girl is approximately four to six years old. The adult male's penis is inserted into the girl's vagina.

61. On or about January 28, 2023, NCMEC received a Cybertip, number 154010151, from MeWe. MeWe provided the following identifiers for the associated subject MeWe account, the SUBJECT ACCOUNT 3:

- E-mail address: gerrybr1681@yahoo.com
- Username: Paullie Walking
- Login IP Address: 35.148.74.1

62. MeWe provided the filename and MD5 Hash Value for the twenty-four (24) uploaded image files, which prompted MeWe to file the Cybertip.

63. MeWe provided the twenty-four (24) image files which were viewed by MeWe and NCMEC that were submitted with the Cybertip. I reviewed the files and determined they were consistent with the definition of child pornography. One of the images is described as follows:

- Filename: i_63d56bdd83cd9f37c3bddee9.jpg
- Incident Date/Time: 1/26/2023 17:29:322 UTC

- MD5 Hash Value: ca1bda2ffe33bdd8f749c282b9715321
- The image is a full color image which shows an infant with an adult male's penis in the infant's open mouth.

64. On or about February 10, 2023 MeWe was served with a federal search warrant issued in the Eastern District of Wisconsin for the contents of SUBJECT ACCOUNT 2 and 3. On or about February 10, 2023 MeWe provided records related to SUBJECT ACCOUNT 2 and 3 in response to the federal search warrant.

65. I reviewed the contents of the records provided by MeWe in response to the search warrant and observed images and videos consistent with child pornography, as well as direct messages between SUBJECT ACCOUNT 2 and 3 and other accounts where SUBJECT ACCOUNT 2 and 3 shared files of child pornography.

66. The profile image for SUBJECT ACCOUNT 2 was an image with file name 63badb5d4eeb85635b6372c4.jpg, which was an image that appeared to be of Brandon Gerry. On or about January 8, 2023, at 16:57:04Z, the user of SUBJECT ACCOUNT 2 sent a message including the number 4144307294. The number is the same as the U.S. Cellular telephone number registered to Brandon Gerry.

67. On or about January 13, 2023, the user of SUBJECT ACCOUNT 2 was engaged in a conversation with an unidentified person through MeWe. At 18:43:43Z, the user of SUBJECT ACCOUNT 2 shared an image with file name: 63c1a65f6d4b7f1db28ac67d.jpg which I viewed and determined is consistent with the definition of child pornography. The image is described as follows:

- The full color image depicts a brown haired child of unknown sex facing away from the camera. The child appeared to be approximately 5 to 9 years of age, based

upon lack of body hair or muscular development. The child was fully nude with the exception of a black and neon green article of clothing over its shoulders. The child was holding onto a yellow pillow. An adult male was had his erect penis inserted into the child's buttocks.

68. On or about January 14, 2023 at 8:10:07Z, the User of SUBJECT ACCOUNT 2 continued the conversation by stating, "He's like 6."

69. On or about January 14, 2023 at 9:38:55Z, the user of SUBJECT ACCOUNT 2 shared an image, with a different user, with file name: 63c2782f3ef54d2bc636715e.jpg which I viewed and determined is consistent with the definition of child pornography. The image is described as follows:

- The full color image depicts a prepubescent male, approximately 4 to 8 years of age, laying on a multi-colored rug. The boy's anus and testicles were clearly visible. The boy's face was not visible in the image. An adult male straddled the boy and his erect penis was visible. The male appeared to have ejaculated onto the boy's back and anus.

70. A The profile image for SUBJECT ACCOUNT 3 was an image with file name 63d23dabe9f43653ee17f9c8.jpg, which was an image that appeared to be of GERRY.

71. On or about January 28, 2023 the user of SUBJECT ACCOUNT 3 was engaged in a conversation through MeWe with an unidentified individual. At 18:26:46Z, the user of SUBJECT ACCOUNT 3 stated, "That pic is my friend who fuck his 4 yo daughter and 6 yo son." At 18:27:21Z, the user of SUBJECT ACCOUNT 3 shared an image with file name

63d5690834e15d2f28db6ad1.jpg which I viewed and determined is consistent with the definition of child pornography. The image is described as follows:

- The full color image depicts a child of an undetermined sex, approximately 3 to 7 years of age. The child is on a bed with its face in a pillow and knees tucked under its body. The child is wearing a pink or light-colored shirt or dress. A fully nude adult male is on his hands and knees with his pelvis directly behind the child's rear.

72. At 18:53:02Z, the user of SUBJECT ACCOUNT 3 shared an image with file name: 63d56f0e34e15d2f28e4d173.jpg which I viewed and determined is consistent with the definition of child pornography. The image is described as follows:

- The full color image depicts a young child, approximately 4 years of age or less, of an undetermined sex. The child's face is partially obscured in the image by an adult hand covering the child's eyes and forehead. The child appears to be seated in a car seat with a dark grey t-shirt or blanket covering the child's torso. An erect male penis is visible and held by another adult hand while inserted in the child's mouth.

73. The user of SUBJECT ACCOUNT 3 shared at least one additional image consistent with the definition of child pornography as the conversation continued. At 18:31:32Z, the user of SUBJECT ACCOUNT 3 stated, "What ages do you like?" At 18:31:44, the user of SUBJECT ACCOUNT 3 stated, "0-10 here." At 18:31:55Z, the user of SUBJECT ACCOUNT 3 stated, "Wanna get a zoom room and watch some." At 18:39:26, the user of SUBJECT ACCOUNT 3 shared the image with file name: 63d56bdd83cd9f37c3bddee9.jpg, which was provided with the NCMEC Cybertip and previously described in this affidavit. At 18:41:13Z, the user of Subject

Account 3 shared a link to a Zoom Video Communications, Inc. website. At 18:52:44Z, the user of SUBJECT ACCOUNT 3 stated, "Normally o do but today I just want baby sex."

Reddit

74. On or about January 31, 2023, NCMEC received a Cybertip, number 154218103, from Reddit. Reddit provided the following identifiers for the associated subject Reddit account, the SUBJECT ACCOUNT 4:

- E-mail address: gerrybr1681@gmail.com
- Username: FrontInteraction3354
- Registration IP Address: 166.181.80.60
- Registration Date/Time: 01-10-2023 07:09:11 UTC
- Upload IP Address: 35.148.74.1
- Upload Date/Time: 01-29-2023 01:10:53 UTC

75. Reddit provided the filename and MD5 Hash Value for the one (1) uploaded file, which prompted Reddit to file the Cybertip. Reddit also stated that this upload was from a Reddit chat message, indicating that the SUBJECT ACCOUNT distributed this image to another account via private chat.

76. Reddit provided the one (1) file which was viewed by Reddit and NCMEC that was submitted with the Cybertip. I reviewed the file and determined it was consistent with the definition of child pornography. The image is described as follows:

- Filename: file
- MD5 Hash Value: e7e6c3026201fbf44aefb11ab597a40d
- The image is a full color image which shows a nude, prepubescent female, sitting with her legs spread on the lap of an adult male. The girl is approximately five to seven years old. The adult male's penis is inserted into the girl's vagina, and he is holding her chest.

77. On or about January 31, 2023, NCMEC received a Cybertip, number 154218094, from Reddit. Reddit provided the following identifiers for the associated subject Reddit account, the SUBJECT ACCOUNT 4:

- E-mail address: gerrybr1681@gmail.com
- Username: FrontInteraction3354
- Registration IP Address: 166.181.80.60
- Registration Date/Time: 01-10-2023 07:09:11 UTC
- Upload IP Address: 35.148.74.1
- Upload Date/Time: 01-29-2023 01:10:53 UTC

78. Reddit provided the filename and MD5 Hash Value for the one (1) uploaded file, which prompted Reddit to file the Cybertip. Reddit also stated that this upload was from a Reddit chat message, indicating that the SUBJECT ACCOUNT 4 distributed this image to another account via private chat.

79. Reddit provided the one (1) file which was viewed by Reddit and NCMEC that was submitted with the Cybertip. I reviewed the file and determined it was consistent with the definition of child pornography. The image is described as follows:

- Filename: file
- MD5 Hash Value: fe895f6875f2284eef279f2feda49722
- The image is a full color image which shows a nude prepubescent girl from the stomach down, lying on her back with her legs spread. The girl is approximately four to six years old. There is an adult male penis inserted into the girl's vagina and a white substance, consistent with semen, on the girl's stomach and vagina.

80. On or about February 3, 2023, NCMEC received a Cybertip, number 154454318, from Reddit. Reddit provided the following identifiers for the associated subject Reddit account, the SUBJECT ACCOUNT 5:

- E-mail address: gerrybr1681@yahoo.com
- Username: cumfilledwb

- Registration IP Address: 64.132.194.156
- Registration Date/Time: 01-31-2023 06:46:03 UTC
- Upload IP Address: 166.181.88.3
- Upload Date/Time: 02-01-2023 09:43:02 UTC

81. Reddit provided the filename and MD5 Hash Value for the one (1) uploaded file, which prompted Reddit to file the Cybertip. Reddit also stated that this upload was from a Reddit chat message, indicating that the SUBJECT ACCOUNT 5 distributed this image to another account via private chat.

82. Reddit provided the one (1) file which was viewed by Reddit and NCMEC that was submitted with the Cybertip. I reviewed the file and determined it was consistent with the definition of child pornography. The image is described as follows:

- Filename: file
- MD5 Hash Value: 7052ca4e5805d2df4085485807073ec9
- The image is a full color image which shows a nude prepubescent male from the stomach down, lying on his back with her legs spread. The boy is approximately four to six years old. There is an adult male between the boy's legs, and the adult male's penis is touching the boy's penis.

83. On or about February 7, 2023 a Preservation Request was served on Reddit for the SUBJECT ACCOUNTS by an Operational Support Technician at FBI Milwaukee.

84. On or about February 10, 2023 Reddit was served with a federal search warrant issued in the Eastern District of Wisconsin for the contents of SUBJECT ACCOUNT 4 and 5. On or about February 16, 2023 Reddit provided records related to SUBJECT ACCOUNT 4 and 5 in response to the federal search warrant.

85. I reviewed the contents of the records provided by Reddit in response to the search warrant and observed images consistent with child pornography, as well as direct messages

between SUBJECT ACCOUNT 4 and 5 and other accounts where SUBJECT ACCOUNT 4 and 5 shared image files of child pornography.

86. SUBJECT ACCOUNT 4 sent multiple messages expressing that the user had a sexual interest in children. These messages included but are not limited to:

- 2023-01-19 09:36:04 UTC: Can't help it but right after I slam I wanna see a kid get fucked by it's dad

- 2023-01-23 09:11:18 UTC: I'm horny af
- 2023-01-23 09:11:31 UTC: And feel like I wanna molest a kid

- 2023-01-26 04:27:41 UTC: Twisted pedo here bro
- 2023-01-26 04:27:55 UTC: I just slammed and I wanna use a toddler with you

- 2023-01-26 13:21:43 UTC: I got vids of dad's fucking there daughters
- 2023-01-29 01:09:50 UTC: As soon as I slam though my dick takes over and wants to fuck some kids

87. SUBJECT ACCOUNT 4 also had multiple conversations with other accounts where the user expressed a sexual interest in children. These message exchanges included (SUBJECT ACCOUNT 4 is in bold):

2023-01-29 18:59:56 UTC FrontInteraction3354	**What's up**
2023-01-29 19:04:33 UTC Sad666Daddy	So you're in the kids right
2023-01-29 19:04:36 UTC Sad666Daddy	Into
2023-01-29 19:04:45 UTC Sad666Daddy	I'm into what I'm into but I just can't understand how someone's in the kids
2023-01-29 19:04:55 UTC Sad666Daddy	Into
2023-01-29 19:05:45 UTC Sad666Daddy	So I'm asking the mind of a pedophile why
2023-01-29 19:08:02 UTC FrontInteraction3354	**Because it's so perverted and wrong that it just feels right. Plus 90% of the time you get to fuck your own kids**
2023-01-29 19:08:15 UTC FrontInteraction3354	**Incest and yng all in one perverted fuck**
2023-01-29 19:08:49 UTC	Don't you think it's wrong for the kid

Sad666Daddy	
2023-01-29 19:09:00 UTC	Because obviously it's not like they have a choice
Sad666Daddy	
2023-01-29 19:09:12 UTC	Rape
Sad666Daddy	
2023-01-29 19:09:17 UTC	Its
Sad666Daddy	
2023-01-29 19:09:52 UTC	I like rapelust.com
Sad666Daddy	
2023-01-29 19:09:57 UTC	Checked that out but still
Sad666Daddy	
2023-01-29 19:10:43 UTC	**I mean of course it's wrong and the poor kids but when I'm high I**
FrontInteraction3354	**could give a damn. Sober I'm not into it at alll**

2023-01-19 08:59:56 UTC	You like kink?
hampstr2854	
2023-01-19 09:00:10 UTC	**Fuck yeah I love kink**
FrontInteraction3354	
2023-01-19 09:00:19 UTC	**N kids**
FrontInteraction3354	
2023-01-19 09:00:30 UTC	What's your favorite?
hampstr2854	
2023-01-19 09:00:42 UTC	How old?
hampstr2854	
2023-01-19 09:01:13 UTC	Your fave kink
hampstr2854	
2023-01-19 09:03:05 UTC	**My favorite is incest**
FrontInteraction3354	
2023-01-19 09:03:21 UTC	**Ages 0-10**
FrontInteraction3354	
2023-01-19 09:03:38 UTC	Mmm...wow
hampstr2854	
2023-01-19 09:03:51 UTC	Boys or girls?
hampstr2854	
2023-01-19 09:04:57 UTC	**Both**
FrontInteraction3354	

88. SUBJECT ACCOUNT 4 shared images consistent with child pornography on more than twenty (20) occasions. One message exchange example is shown below (SUBJECT ACCOUNT 4 is in bold):

2023-01-26 12:44:23 UTC	**FrontInteraction3354**	**Hzfeqfr4dfea1.png- Description: Full color image of a prepubescent girl, approximately five to seven years old, lying on her back. An adult male is holding the girl's legs up, and her pants are pulled down around her knees, exposing her nude vagina and anus. The adult male's penis is touching the girl's nude vagina.**
2023-01-26 12:44:33 UTC	**FrontInteraction3354**	**Fuck man**
2023-01-26 12:44:36 UTC	InternationalFact688	53 str8 here but love spun naked fun with buds
2023-01-26 12:44:51 UTC	**FrontInteraction3354**	**Fuck yeah**
2023-01-26 12:45:07 UTC	**FrontInteraction3354**	**Perv on kids**
2023-01-26 12:45:29 UTC	InternationalFact688	Where you located?
2023-01-26 12:45:33 UTC	**FrontInteraction3354**	**Wi**
2023-01-26 12:45:35 UTC	**FrontInteraction3354**	**U**
2023-01-26 12:45:39 UTC	InternationalFact688	Maryland
2023-01-26 12:45:43 UTC	**FrontInteraction3354**	**Dick pic?**
2023-01-26 12:46:00 UTC	InternationalFact688	This is my laptop. Nothing on here
2023-01-26 12:46:25 UTC	InternationalFact688	But next time im fired up I'll send you all my pics real time
2023-01-26 12:46:29 UTC	InternationalFact688	Chat, cam
2023-01-26 12:46:33 UTC	**FrontInteraction3354**	**Damn I'd like to imagine your dick opening a 5 yo hole**
2023-01-26 12:46:37 UTC	InternationalFact688	really like in person
2023-01-26 12:46:55 UTC	**FrontInteraction3354**	**Cool**
2023-01-26 12:47:15 UTC	**FrontInteraction3354**	**1pn72f8ndfea1.png- Description: Full color image of a completely nude prepubescent girl, approximately three to five years old on her knees, face down facing away from the camera. The girl's ankles are tied with rope and her legs are spread so her vagina and anus are exposed.**

89. SUBJECT ACCOUNT 5 sent multiple messages expressing that the user had a sexual interest in children. These messages included but are not limited to:

- 2023-02-01 09:47:10 UTC: Is it a pedo dick
- 2023-02-01 09:47:13 UTC: Mine is

- 2023-02-01 10:54:09 UTC: I have lots of child porn

- 2023-02-01 15:25:16 UTC: Slamming it turns me into a pedophile

- 2023-02-01 16:39:46 UTC: Especially a yng bald [pussy] filled with pedo cum

- 2023-02-01 10:53:08 UTC: And I like to get freaky as fuck. Huge perv love incest and kids

90. SUBJECT ACCOUNT 5 also had multiple conversations with other accounts where the user expressed a sexual interest in children. These message exchanges included the following (SUBJECT ACCOUNT 5 is in bold):

2023-02-02 11:32:50 UTC	**What kinda of perv do you like**
2023-02-02 23:48:54 UTC	Adolescent boys, just old enough to cum, gay incest, you?
2023-02-02 23:53:56 UTC	**Sane but I like boy s n girls age p10**
2023-02-02 23:55:59 UTC	**O-13**

91. SUBJECT ACCOUNT 5 shared images consistent with child pornography on multiple occasions. Examples of the images shared by the SUBJECT ACCOUNT 5 are below:

- 2023-02-01 10:23:04 UTC: This is a full color image of a prepubescent male, approximately eight to ten years old. There is an adult male's penis in the boy's mouth and a white substance consistent with semen is dripping out of the boy's mouth.

- 2023-02-01 09:50:50 UTC: The image is a full color image which shows a nude, prepubescent female, sitting with her legs spread on the lap of an adult male. The girl is approximately five to seven years old. The adult male's penis is inserted into the girl's vagina, and he is holding her chest. This image was provided in one of the Cybertips described above.

Surveillance

92. On or about February 21, 2023 a team of FBI Special Agents (Agents) conducted surveillance at the SUBJECT PREMISES. Upon arrival at the SUBJECT PREMISES, at approximately 8 AM, Agents observed the SUBJECT VEHICLE parked in a parking spot at the apartment complex.

93. At approximately 1:18 PM Agents observed GERRY exit the building which contains the SUBJECT PREMISES, GERRY walked to the SUBJECT VEHICLE and then returned into the apartment building which contains the SUBJECT PREMISES.

94. On or about February 23, 2023 Agents were conducting surveillance at the SUBJECT PREMISES. At approximately 9:40 AM Agents observed the SUBJECT VEHICLE approach the SUBJECT PREMISES and park. GERRY exited the SUBJECT VEHICLE and entered the apartment building containing the SUBJECT PREMISES.

95. Based upon the provided information, there is probable cause to believe the user of the collective SUBJECT ACCOUNTS has received, uploaded, or distributed more files of child pornography, and that GERRY was the user of those accounts. There is probable cause to believe that GERRY's electronic devices will contain evidence of violations of federal criminal law and those devices could be found in the SUBJECT VEHICLE, in the SUBJECT PREMISES or on the person of GERRY.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

96. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers, cellular telephones, and other electronic storage devices (collectively electronic storage devices) have dramatically changed the way in which individuals interested in child pornography interact with each other. Electronic storage devices basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a device by simply connecting the camera to the electronic storage device. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store terabytes of data, which provides enough space to store thousands of high-resolution photographs. Video recorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the video recorder to a computer. Many electronic storage devices (e.g., computers, cellular telephones, and tablets), have cameras built into the device which allows users to create and store still and video images on the device. Moreover, if the device has internet connectivity, users can distribute still and video images from the device.

c. Internet-enabled electronic storage devices can connect to other internet-enabled devices the world over. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically

changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to an internet-enabled electronic storage device. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, electronic storage devices are the preferred method of distribution and receipt of child pornographic materials.

d. Electronic storage devices are the ideal repository for child pornography. The amount of information that an electronic storage device can hold has grown exponentially over the last decade. Electronic storage devices can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on a computer or other electronic storage device. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Many electronic storage devices can easily be concealed and carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Google, among

others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any internet-enabled electronic storage device. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's electronic storage device in most cases.

g. As is the case with most digital technology, communications by way of electronic storage device can be saved or stored on the device. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, an electronic storage device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

h. Based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

97. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage.

98. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

99. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who transport, distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

d. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices using forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

e. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Such individuals prefer not to be without their child pornography for any prolonged period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if an individual, uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in the SUBJECT PREMISES, SUBJECT VEHICLE or a device located on GERRY, as set forth in Attachment A.

46. I believe the resident sharing child pornography at the SUBJECT PREMISES likely displays characteristics common to individuals who possess, access with intent to view, and distribute child pornography based on his history of distributing child exploitation material as set forth in this affidavit.

47. Based on my training and experience, I believe that a ping and cell-site simulator are likely to uncover evidence of this crime in that the ping and cell-site simulator will assist me in locating the devices used to commit the above-described crimes. Additionally, based on my

training and experience, individuals who commit the above-described crimes frequently hide the devices used to commit said crimes, and the cell-site simulator will assist me in locating the devices.

CONCLUSION

48. I respectfully request that this Court issue a search warrant for the location, vehicle and search of person described in Attachment A authorizing the seizure and search of the items described in Attachment B.

❒ Original ❒ D

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
212 S Univeristy Dr. #6, West Bend, WI 53095; silver 2018 Buick, VIN KL4CJCSB0JB524629, WI plate ANG1780; person of Brandon Gerry, DOB 12/5/1984; (See Attachments)

Case No. 23 MJ 52

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before 3/13/2023 *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable William E. Duffin.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 2/27/2023 at 12:02 PM

William E. Duffin
Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

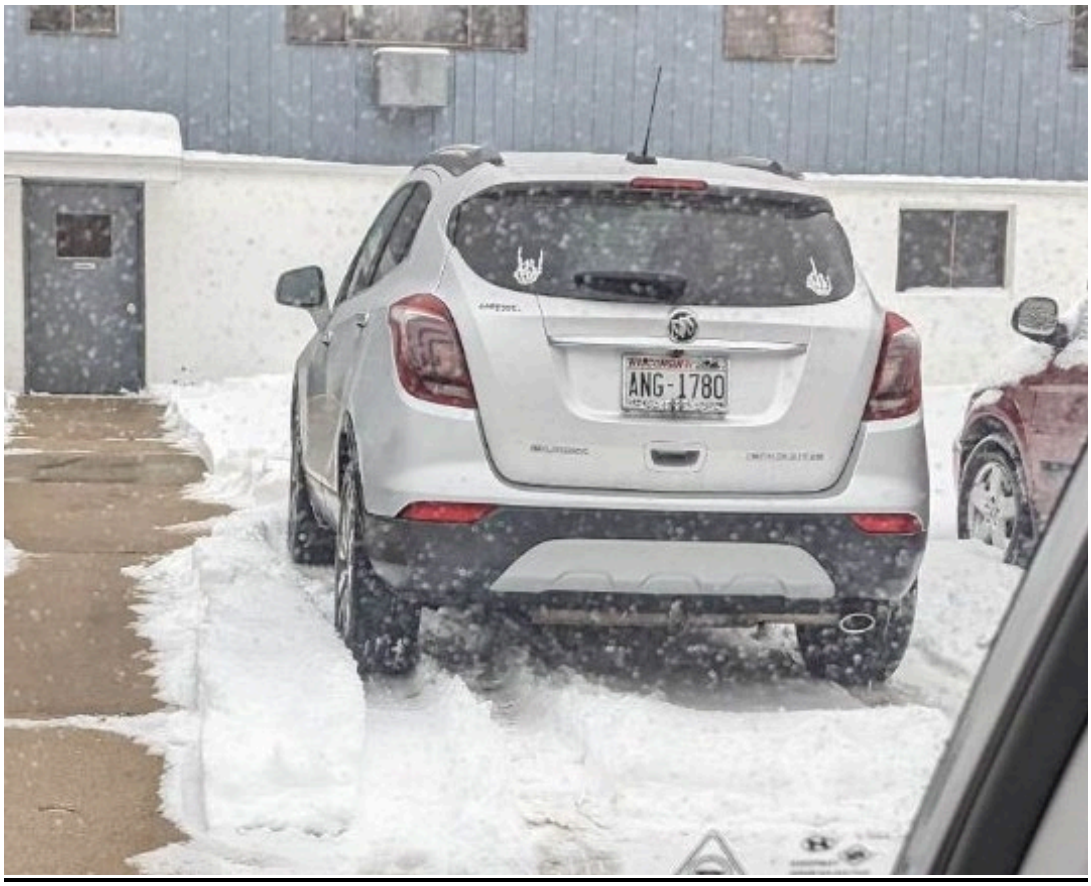
ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

(1) 212 S UNIVERSITY DR, APT 6, WEST BEND, WI 53095 (photo below) limited to the apartment of Brandon Gerry, the apartment labeled "6". The apartment building has a stone veneer around the first floor, and blue siding around the top floor. There is an entrance on the front facing the street. There is also an entrance on the back, with a walkway to the parking lot, there is a basement level which walks out to the parking lot.

(2) silver 2018 Buick, VIN KL4CJCSB0JB524629, Wisconsin license plate ANG1780 (photo below)

(3) the person of Brandon Gerry, DOB 12/5/1984.


ANG-1780

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Cell phones, computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of any device by use of the computer or by other

means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment.

13. Any and all visual depictions of minors.

14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. For any electronic storage device, computer hard drive, electronic device, or other physical object upon which electronic information can be recorded (hereinafter, "electronic storage device") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

    a. evidence of who used, owned, or controlled the electronic storage device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the electronic storage device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. evidence of the lack of such malicious software;

    d. evidence indicating how and when the electronic storage device was accessed or used to determine the chronological context of electronic storage device access, use, and events relating to crime under investigation;

    e. evidence indicating the electronic storage device user's location and state of mind as it relates to the crime under investigation;

    f. evidence of the attachment to the electronic storage device of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage device;

h. evidence of the times the electronic storage device was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage device;

j. documentation and manuals that may be necessary to access the electronic storage device or to conduct a forensic examination of the electronic storage device;

k. contextual information necessary to understand the evidence described in this attachment.

17. Records and things evidencing the use of the Internet Protocol addresses to communicate with the internet, including:

a. routers, modems, and network equipment used to connect electronic storage devices to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of Brandon Gerry to the Touch

ID sensor of device(s) or scan for facial recognition, such as an iPhone. Android, or Tablet, found at the premises for the purpose of attempting to unlock the device via fingerprint or facial recognition in order to search the contents as authorized by this warrant. If facial recognition is required, Brandon Gerry will remain still and look, with eyes open, at the camera for any devices seized in connection if this warrant for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.